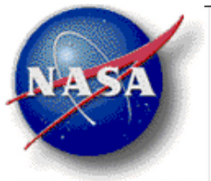


A systems modeling approach for risk management of command file errors

Leila Meshkat

Jet Propulsion Laboratory, California Institute of Technology

Outline

- Why Command Errors?
- Approach
- Use Case – Anomaly Investigation
- Summary of Observations
- Use Case Objective
- Sample Anomaly Model(s)
  - BBN model
  - PRA model for command generation process
  - PRA model for sequence of activities
- Data Gaps for Risk Management
- Conclusions

Why Command Errors?

- Often the symptom of some kind of imbalance or inadequacy
  - within the system that comprises the hardware & software used for command generation and/or
  - the team involved in this endeavor.
- Era of enhanced collaboration with other NASA centers and commercial partners
  - systems become more and more complex
  - it is imperative to formally model and analyze command generation systems in order to manage the risk of command file errors.

Approach

- Combined Bayesian Belief Network and Probabilistic Risk Assessment Models.
  - BBN model of commanding errors
    - These models take into consideration all the possible causes for commanding errors.
    - They use probabilistic reasoning to determine the relative likelihood of each cause.
    - They are used as an aid to the designer in understanding system sensitivities.
  - Probabilistic Risk Assessment Models of Command Generation Process
    - These models take into consideration the causes of failure during command generation.
    - The human related tasks can fail due to human errors. Probability of these errors are assessed using human reliability data banks from the nuclear industry.

Use Case – Anomaly Investigation

- Bayesian Belief Network Models:
  - For the use case in this study:
    - Each anomaly is examined, its' root causes identified in the model and two key scenarios are examined.
      - Scenarios where root causes are present.
      - Scenario where the root cause eliminated with corrective action is no longer present.
      - The probability of commanding error in each case is assessed and compared.
- Probabilistic Risk Assessment Models:
  - Probability of error path that led to anomaly is computed, purely with consideration of human error probabilities.
  - Note that command generation process errors fall under the category of "Process Compliance" root causes in the BBN model.
- Furthermore, the PRA modeling approach is used to represent and analyze sequence of seemingly unrelated activities that lead to commanding errors.
  - That was the case for one of the anomalies.

Summary of Observations

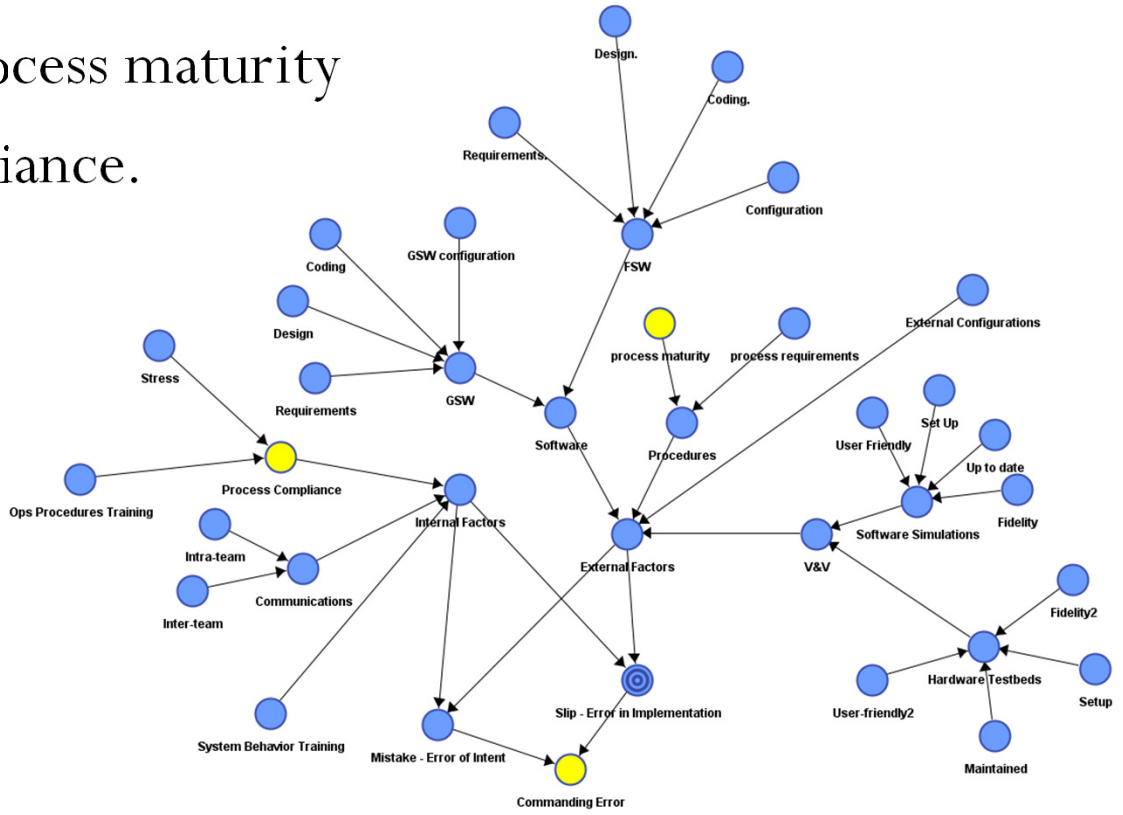
- The anomalies studied were caused due to the following:
  - Inadequate Procedures
    - Process maturity or incomplete process requirements.
  - Lack of Process Compliance.
  - Lack of Understanding of System Behavior/States.
    - Low fidelity of software simulations. (not clearly communicating state of the system.)
  - Inadequate Communication
    - Inter-team or Intra-team communications.
- Most corrective actions address the "Procedures" part of the problem.
  - Although in some instances creating and following clear procedures prevents errors due to lack of understanding system behavior or states of the system, this issue is not addressed directly in the corrective actions.
  - Corrective actions to improve communications or process compliance are not made explicitly.

Use Case Objective

- Determine an approach for reducing Commanding errors
  - Determine the causes of the errors
  - Different error types and sequences
  - Additional assurance
    - Data structure needs
  - Validate effectiveness to prevent errors.
    - Implementation needs

Sample Anomaly Model- BBN Model

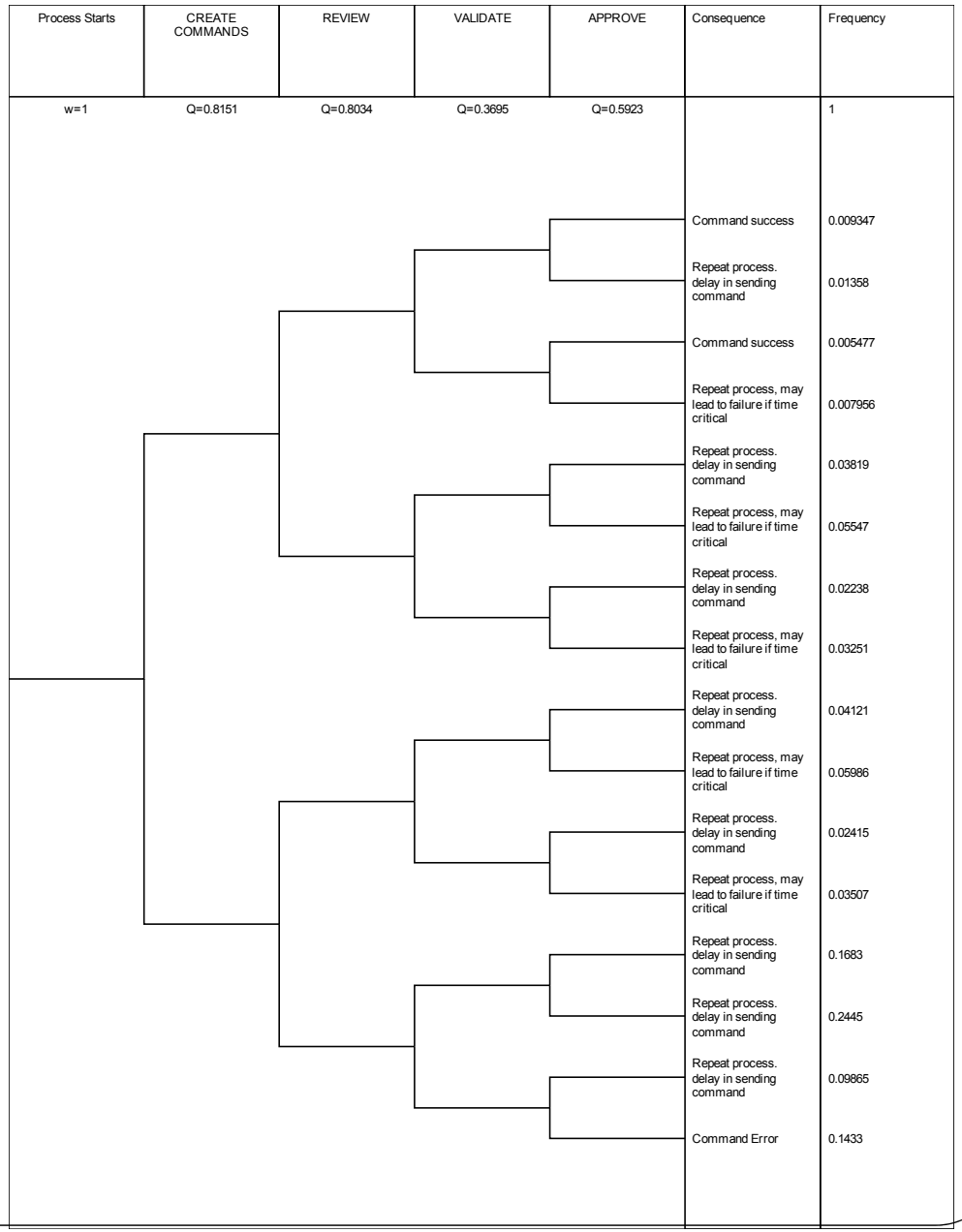
- The command to change to the proper mode was not in sequence. If the STL data had been reviewed, this error would have been caught.
- Error due to lack of process maturity and lack of process compliance.
- Corrective action is to improve procedures.
- This will reduce the Chances of such errors From 0.22 to 0.18



Sample PRA Model : Command Generation Process

Command to change to proper mode not in sequence

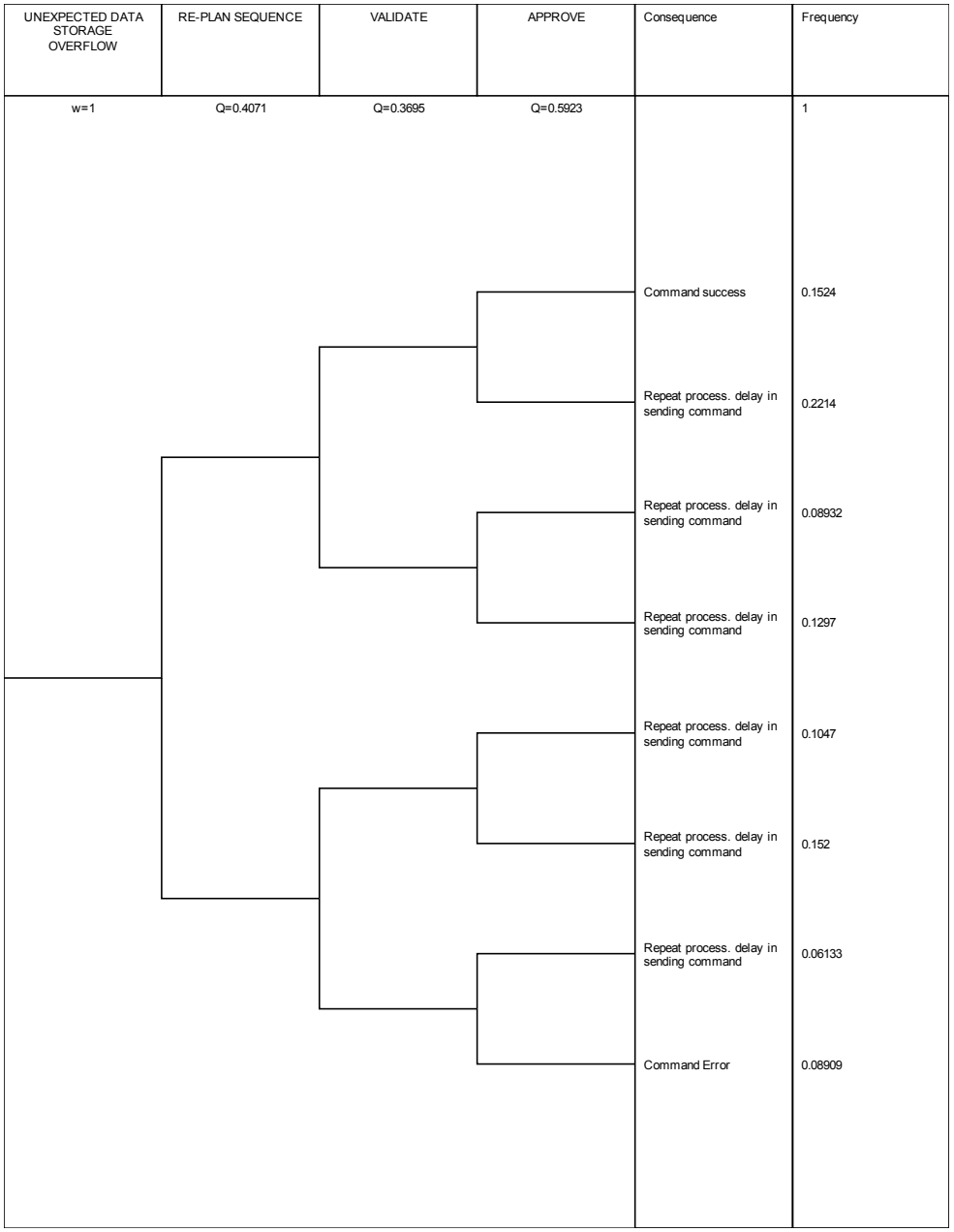
- There's an error (omission) when the command is created.
- It isn't caught during review.
- It isn't caught during validation.
- It isn't caught during approval cycle.
- There's an 0.1433 chance that it will fall through all these cracks.



Sample PRA Model : Accident Scenario

Command to Delete Packet Violated Flight Rules

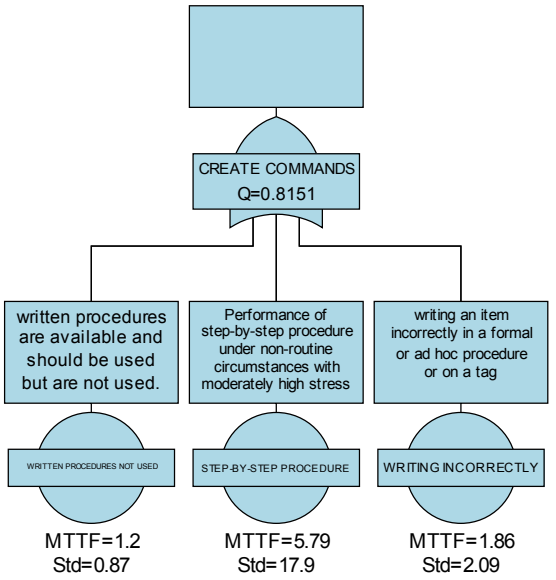
- There was an unexpected data storage overflow
- This resulted in a change in original planned sequences.
- Plans violated flight rules.
- Flight rule violation was not flagged prominently during review/approval portion of the process.
- There is an 0.089 chance of this path occurring.



Sample PRA Model : Command Generation Process

Command to change to proper mode not in sequence

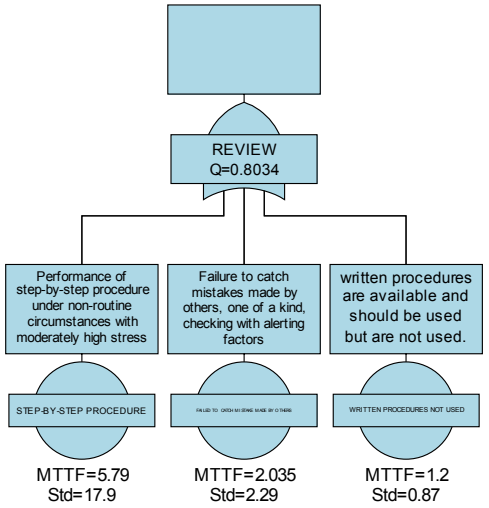
- During creation:
  - Written Procedure was available but not used OR
  - Wrote an item incorrectly in a formal or ad-hoc procedure OR
  - Made an error while performing a step-by-step procedure under non-routine circumstances with moderately high stress



Sample PRA Model : Command Generation Process

Command to change to proper mode not in sequence

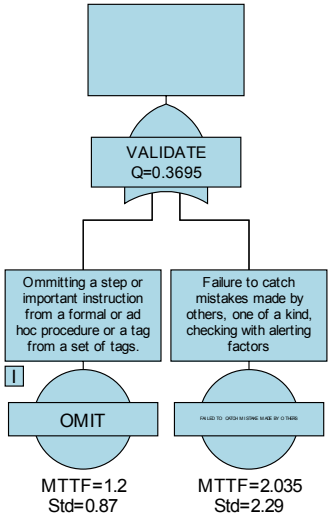
- During creation:
  - Written Procedure was available but not used OR
  - Failed to catch mistakes made by others OR
  - Made an error while performing a step-by-step procedure under non-routine circumstances with moderately high stress



Sample PRA Model : Command Generation Process

Command to change to proper mode not in sequence

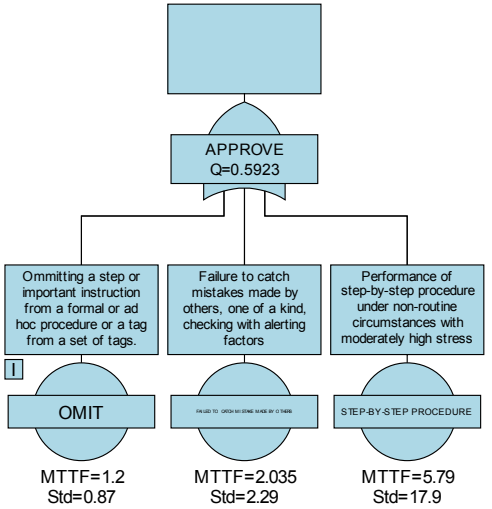
- During Validation:
  - Omitted a step or important instruction from a procedure OR
  - Failed to catch mistakes made by others



Sample PRA Model : Command Generation Process

Command to change to proper mode not in sequence

- During Approval:
  - Omitted a step or important instruction from formal or ad hoc procedure OR
  - Failed to catch mistake made by others OR
  - Made an error while performing a step-by-step procedure under non-routine circumstances with moderately high stress



Data Gaps for Risk Management

- Data Structure
  - A structured approach for anomaly identification, assessment and mitigation.
  - Structure needs to enable inputting:
    - Sequence of events
    - Rationale for each event
    - Dependencies
- Process Improvement Implementation Needs
    - Each flight project is different.
    - Same general BBN model can be customized for different projects.
    - Need information about each of the nodes in the BBN specific for that project.
      - Questionnaires already exist.

Conclusions

- The main cause of commanding errors is often (but not always) due to procedures.
  - Either lack of maturity in the processes, incompleteness of requirements or lack of compliance to these procedures.
- Other causes of commanding errors include lack of understanding of system states, inadequate communication, and making hasty changes in standard procedures in response to an unexpected event.
- In general, it's important to look at the big picture prior to making corrective actions.
- In the case of errors traced back to procedures, considering the reliability of the process as a metric during its' design may help to reduce risk.
  - This metric is obtained by using data from Nuclear Industry regarding human reliability.
- A structured method for the collection of anomaly data will help the operator think systematically about the anomaly and facilitate risk management.
- Formal models can be used for risk based design and risk management.
- A generic set of models can be customized for a broad range of missions.